



# Department of Homeland Security Daily Open Source Infrastructure Report for 02 July 2007

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The New York Times reports a smuggling tunnel freshly excavated under the border with Mexico was sealed Friday, June 29, after a joint raid by United States and Mexican authorities. (See item [13](#))
- The Associated Press reports some U.S. airports will tighten security in response to terrorist incidents in Britain; the U.S., however, is not raising its terror alert status at this time. (See item [15](#))
- CNN reports a man who allegedly stored nearly 1,500 pounds of potassium nitrate and other chemicals in his Staten Island home and a nearby storage facility was charged with reckless endangerment Friday, June 29. (See item [42](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *June 29, Tribune News (CA)* — **More nuclear reactors may be built in California, reversing thinking of just two years ago.** Executives with California's two nuclear power utilities told the state Energy Commission on Thursday, June 28, that they are considering the possibility of building new nuclear plants as a means of meeting the state's future energy needs. Jack Keenan

with Pacific Gas and Electric Co. and Gary Schooyan of Southern California Edison said new nuclear power generation is part of the mix of energy sources they are considering using as they do long-range planning. "We need to keep that option open to us," Keenan said. "We are studying it very hard." PG&E operates San Luis Obispo County's Diablo Canyon nuclear power plant, and Southern California Edison operates the San Onofre nuclear generating station near Carlsbad. The statements Thursday mark a shift since 2005, when the Energy Commission last held hearings on the future of nuclear power in the state. At that time, PG&E and Edison officials expressed little interest in new nuclear power stations. PG&E is also looking at the possibility of new reactors out of the state that could serve California customers, similar to the way Palo Verde nuclear power plant in Arizona provides power for Southern California.  
Source: <http://www.sanluisobispo.com/news/local/story/80204.html>

2. *June 28, Associated Press* — **Energy security looms large as NATO meets with eastern neighbors in Macedonia.** NATO should play a greater role protecting its members' energy security, the alliance's top diplomat said Thursday, June 28, amid concerns that fuel supplies are increasingly at risk from threats ranging from terrorist attacks to supply cuts by disgruntled exporters. "NATO has role to play in this field," Secretary General Jaap de Hoop Scheffer told a gathering of ministers and senior diplomats from almost 50 allied and partner nations. NATO allies have mixed views on the alliance's role in protecting energy resources. Some have pushed for NATO to consider a military role helping protect pipelines, oil platforms and sea routes bringing oil and gas to Europe and North America. Poland, which is heavily dependent on Russian oil and gas imports, has suggested a pact to support allies whose supplies are threatened. France — traditionally wary of extending the trans-Atlantic alliance's role — and others have been reluctant to have NATO take on new energy security tasks. De Hoop Scheffer said NATO should work with other international organizations to "add value" to efforts to "protect allies' security interests and strengthen the security of energy infrastructure."  
Source: <http://www.iht.com/articles/ap/2007/06/28/europe/EU-GEN-NATO-Eastern-Neighbors.php>

3. *June 28, Providence Journal (RI)* — **High heat triggers no-shutoff utility rule.** A new Rhode Island state rule that prohibits utility shutoffs on extremely hot days was triggered for the first time Wednesday, June 27. A moratorium on heat-related shutoffs, which was implemented by the Public Utilities Commission in March, went into effect at 10:21 a.m. EDT when the National Weather Service issued a "heat advisory" for Southern New England. The rule says that state-regulated public utility companies cannot terminate the service of any residential customer for nonpayment on days in which the National Weather Service has issued a heat advisory or excessive heat warning for Rhode Island. National Grid was performing shutoffs Wednesday morning before the advisory was issued, said David Graves, spokesperson for the company. The company monitors the National Weather Service's Website and when it became aware of the advisory, it notified crews by radio or cell phone to halt shutoffs, Graves said. The heat-related shutoff moratorium arose out of efforts by the George Wiley Center, an antipoverty group in Pawtucket, to ban shutoffs during extremely hot weather. The number of shutoffs so far this year is the second highest in a decade.  
Source: [http://www.projo.com/news/content/bz\\_hot\\_weather\\_shutoff\\_ban\\_06-28-07\\_NF6635A.2679c6f.html](http://www.projo.com/news/content/bz_hot_weather_shutoff_ban_06-28-07_NF6635A.2679c6f.html)

4.

*June 27, Department of Energy* — **DOE provides up to \$51.8 million to modernize U.S. electric grid System.** U.S. Department of Energy (DOE) Secretary Samuel W. Bodman Wednesday, June 27, announced that DOE will provide up to \$51.8 million for five cost-shared projects that will help accelerate much-needed modernization of our Nation's electricity grid. This research will advance the development and application of high-temperature superconductors, which have the potential to alleviate congestion on an electricity grid that is experiencing increased demand from consumers. The selected projects will help advance the future generation of power delivery equipment and aid the development of a highly efficient electricity grid system for the nation. Two of the research projects will help increase reliability and efficiency of power delivery cables, and the remaining three projects will place an emphasis on fault current limiters. Selected projects include a 13.8-kilovolt superconducting cable to connect two existing substation sites and solve a real-world electrical load problem near downtown New Orleans; second-generation, high-temperature superconductor cables and a single-phase prototype cable in the Long Island Power Authority power grid; development and in-grid testing of a three-phase high-voltage, 115-kilovolt fault current limiter by using second-generation wire; among other projects.  
Source: <http://www.energy.gov/news/5180.htm>

5. *June 27, Detroit Free Press* — **State regulators issue warning on utility line theft.** The Michigan Public Service Commission has issued a consumer alert on the problem of utility cable theft. The state regulatory agency said copper cable theft is a growing problem across Michigan, as global demand for the commodity has resulted in the price of copper increasing nearly six fold in the last five years to more than \$3 a pound. Michigan Public Service Commission press release:  
[http://www.michigan.gov/documents/mpsc/coppertheft\\_200636\\_7.pdf](http://www.michigan.gov/documents/mpsc/coppertheft_200636_7.pdf)  
Source: <http://www.freep.com/apps/pbcs.dll/article?AID=/20070627/BUSINESS06/70627022/1019>

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

6. *June 29, KTBS (LA)* — **Crew cuts gas line.** Two houses in Benton, LA, were evacuated Friday, June 29, after town workers cut a natural gas line. No one was injured and there was no explosion. There were homes in the immediate vicinity of the leak but the residents were away when the line was cut. The town crew was cleaning out ditches when a piece of equipment accidentally hit the gas line.  
Source: [http://www.ktbs.com/viewnews.cfm?news\\_id=2694&zone\\_id=12&title=Crew%20cuts%20gas%20line;%20two%20houses%20evacuated](http://www.ktbs.com/viewnews.cfm?news_id=2694&zone_id=12&title=Crew%20cuts%20gas%20line;%20two%20houses%20evacuated)

[[Return to top](#)]

## **Defense Industrial Base Sector**

7. *June 29, Government Accountability Office* — **GAO-07-273: Defense Contracting: Improved Insight and Controls Needed over DoD's Time-and-Materials Contracts**

**(Report).** Under time-and-materials contracts, payments to contractors are made based on the number of labor hours billed at hourly rates and, if applicable, other direct costs. Because of the risk they pose to the government, their use is supposed to be limited to cases where no other contract type is suitable. The Government Accountability Office (GAO) was asked to identify trends in the Department of Defense's (DoD) obligations under time-and-materials contracts; analyze what DoD is buying under these contracts; assess why DoD is using them and whether actions are being taken to ensure that they are used only when no other contract type is suitable; evaluate DoD's monitoring of contractor performance; and determine the differences between the labor rates prime contractors bill DoD and the rates in their subcontracts. GAO is recommending that DoD require more diligence in justifying the use of certain types of time-and-materials contracts, analyze the use of time-and-materials on indefinite-quantity contracts to ensure that it does not become the default contract type, and require monitoring plans to reflect the risks inherent in this contract type.

Highlights: <http://www.gao.gov/highlights/d07273high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-273>

8. *June 29, Government Accountability Office* — **GAO-07-304: Military Base Closures: Projected Savings from Fleet Readiness Centers Likely Overstated and Actions Needed to Track Actual Savings and Overcome Certain Challenges (Report).** The 2005 Base Realignment and Closure (BRAC) recommendation to establish fleet readiness centers was expected to yield more savings than any other of the 2005 BRAC recommendations. To achieve these savings the Navy plans to integrate civilian depot personnel to complete some repairs at intermediate maintenance departments to reduce aviation maintenance costs. This report, prepared under the Comptroller General authority to conduct evaluations on his own initiative, is one in a series of reports related to the 2005 BRAC recommendations. The Government Accountability Office's (GAO) objectives were to (1) analyze the reasons for changes in costs and savings estimates since the recommendation was approved, and (2) identify challenges in implementing this BRAC recommendation. GAO analyzed Navy and BRAC Commission costs and savings estimates and interviewed officials at the Naval Air Systems Command and at three fleet readiness centers. GAO is making recommendations for the Navy to adjust its business plan to include only savings directly related to implementing this BRAC recommendation and to monitor actual savings realized as the recommendation is implemented. In commenting on a draft of this report, the Department of Defense concurred with GAO's recommendations.

Highlights: <http://www.gao.gov/highlights/d07304high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-304>

[\[Return to top\]](#)

## **Banking and Finance Sector**

9. *June 29, Internetnews.com* — **iPhone hype brings out the iPhishermen.** Where there's a hot market, there's a scam. As the hype for the iPhone approaches that of Paris Hilton's release from jail, McAfee's SiteAdvisor has noticed an uptick in scam artists using some of the very tools we trust, like Google, in an attempt to cash in on the mania. "When you see something with the frenzy the iPhone has, that's where you'll see the scammers out in force," Shane Keats of McAfee told internetnews.com. For example, a Google (Quote) search for "iphone" yielded two advertisers for "free iPhones." Should you be foolish enough to sign up with these guys and

give them your e-mail address, you're going to get a lot of spam but no iPhone. SiteAdvisor took the bait. It signed up with easyfreecellphones.com and ended up with an average of 66 e-mails a week. Signing up at giveawaycafe.com was far worse, yielding 511 e-mails per week. McAfee's analysis shows that these sites use bait-and-switch tactics, where you are asked to complete three, four, even five "sponsor offers," such as applying for a credit card, start a student loan consolidation, or a subscription, and often with reputable companies like eBay and Netflix.

Source: <http://www.internetnews.com/security/article.php/3686256>

10. *June 29, Finextra* — **Amex hit by technical glitches.** American Stock Exchange (Amex) was hit by a technical glitch as it opened for trading Thursday morning, June 28, that forced it to shut down for about 45 minutes, marking the second fall over at the exchange in as many weeks. According to press reports the most recent problem resulted from mismatched ticker symbols on an exchange server. This affected trading in equities and exchange traded funds, but options trading was unaffected. Last week Amex suffered technical glitches with a platform it is phasing out, which led to a halt in trading of stocks and exchange traded funds.

Source: <http://finextra.com/fullstory.asp?id=17115>

11. *June 29, InformationWeek* — **E-mail attacks target business executives.** Cyberattackers know how to follow the money, which is why they often set their sights on companies that are rich with customer data that can be sold online to other attackers and to scammers. Now it's getting personal, with top-level business executives, including CEOs, presidents, CIOs, and CFOs, finding themselves being directly targeted by e-mails containing malicious Trojans. MessageLabs, in its June intelligence report, revealed Thursday, June 28, it has intercepted more than 500 targeted attacks that used an e-mail with a Microsoft Word document attached that contains embedded executable code. All of the attacks targeted senior executives across a number of organizations, the e-mail security managed-service provider said. When opened, the executable code activated the Trojan. The e-mails' subject lines typically use words that refer to some current world event or news story. Some of these malicious e-mails are made to look like legitimate e-mails distributed to find leads in the case of a missing British girl. The e-mails also contained a PowerPoint file with highly specialized code for downloading malware onto users' computers. This attack is reminiscent of the recent StormWorm attack, which referenced the stormy weather conditions present throughout most of Europe at the time.

Source: [http://www.informationweek.com/software/showArticle.jhtml;jsessionid=PXEWBFI3ISJMQSNDLOSKHSCJUNN2JVN?articleID=20000171\\_5](http://www.informationweek.com/software/showArticle.jhtml;jsessionid=PXEWBFI3ISJMQSNDLOSKHSCJUNN2JVN?articleID=20000171_5)

[[Return to top](#)]

## **Transportation and Border Security Sector**

12. *July 01, CNN* — **UK on alert after airport attack.** British police searched houses and made arrests Sunday, July 1, as the country remained on "critical" terror alert after an attack on a Scottish airport and the discovery of two car bombs aimed at killing hundreds of people in London. Prime Minister Gordon Brown, in a nationally televised address warned Britons they faced a "long-term and sustained" threat to security but vowed that his countrymen would not yield to intimidation. In Scotland, officers swooped on a "number of houses" in an operation they said was linked to both Saturday's airport attack and the London bombs. Earlier Sunday,



two people were arrested in Cheshire, England, in connection with the incidents, police confirmed. Police sources linked the airport attack to the failed London bomb plots and said they had traced the cars found in the capital back to Glasgow. The United Kingdom raised its terrorism threat level to "critical," the highest level possible, meaning attacks are imminent, after Saturday's incident in which a blazing car was driven into the terminal entrance at Glasgow airport. The Glasgow attack brought the airport to a standstill, with flights grounded and many passengers stuck for hours on the tarmac. Security was raised at other airports worldwide.

Source: <http://www.cnn.com/2007/WORLD/europe/07/01/london.alert/index.html>

13. *June 30, New York Times* — **Smuggling tunnel is found on Arizona–Mexico border.** A smuggling tunnel freshly excavated under the border with Mexico was sealed Friday, June 29, after a joint raid by United States and Mexican authorities. The cramped and wandering tunnel, which connected two homes on opposite sides of the border had no ventilation, but it was outfitted with lights and at least one drainage pump, officials from Immigration and Customs Enforcement and the Drug Enforcement Administration said at a news conference here. It was thought to have been intended for drug smuggling. State police from Sonora, Mexico, arrested five people in the house on the Mexican side of the border, where the digging was initiated, said Terry E. Kirkpatrick, acting assistant agent in charge for the drug enforcement agency. The house on the United States side was under rental but not occupied, he said. Acting on intelligence tips, American agents had been watching the two houses since April 17. No smuggling had been done through the tunnel, Kirkpatrick said. Kirkpatrick noted that the tunnel did not use the network of storm drainage pipes that smugglers have dug into in the past. He said its crude construction revealed a new strategy by drug smugglers.

Source: <http://www.nytimes.com/2007/06/30/us/30tunnel.html>

14. *June 30, Department of Homeland Security* — **DHS: Statement by Secretary Chertoff.** Department of Homeland Security (DHS) Secretary Michael Chertoff said in a statement on Saturday: "We have been in close contact with our counterparts in the UK regarding today's incident at the Glasgow airport and yesterday's car bomb discoveries in London. Our law enforcement and intelligence officials are closely monitoring the ongoing investigations. The senior leadership of the U.S. government has been meeting on these issues both yesterday and today. DHS and the FBI have provided updates and protective measures guidance to our state and local homeland security and law enforcement partners. At this point, I have seen no specific, credible information suggesting that this latest incident is connected to a threat to the homeland. We have no plans at this time to change the national threat level, although we remind everyone that the aviation threat level has been raised to orange since last fall. However, in an abundance of caution during this holiday period, DHS will be implementing plans to increase our security measures at U.S. airports, mass transit and other transportation facilities. Some of these measures will be visible; others will not..."

Source: [http://www.dhs.gov/xnews/releases/pr\\_1183233198811.shtm](http://www.dhs.gov/xnews/releases/pr_1183233198811.shtm)

15. *June 30, Associated Press* — **U.S. to increase some airport security after British scares.** Some U.S. airports will tighten security in response to possible terrorist incidents in Britain, the White House said Saturday, June 30. The U.S., however, is not raising its terror alert status, President Bush's spokesperson, Tony Snow, said. The Transportation Security Administration (TSA) has taken steps to raise alertness at some airports, Snow said. More TSA agents will be

posted outside some terminals, Snow said. "There will be some inconvenience of passengers in terms of longer wait times," Snow said. Meanwhile, police stepped up curbside patrols with canine units at Hartsfield–Jackson Atlanta International Airport. The Port Authority of New York and New Jersey, which operates Newark Liberty in New Jersey and John F. Kennedy and LaGuardia airports in New York, took "a number of measures as we always do to respond to security situations immediately," spokesperson Steve Coleman said. Operations at Miami International Airport went on heightened alert through at least the Fourth of July.

Source: [http://www.usatoday.com/news/nation/2007-06-30-us-reaction\\_N.htm](http://www.usatoday.com/news/nation/2007-06-30-us-reaction_N.htm)

16. *June 29, Associated Press* — **With storm problems, Delta cancels 200 flights to avoid delays.** Delta Air Lines canceled about 200 flights to and from several northeastern airports Thursday, June 28, to minimize delays caused by heavy thunderstorms forecast across the region. Atlanta-based Delta said it made an early call to cancel the flights in hopes of giving at least 12-hours notice to affected passengers via automated e-mail and cell phone messages or calls from reservations staff. Passengers could ask for refunds or switch to other flights for no additional fees. The airline said flights were canceled in New York; Newark, NJ; Hartford, CT; Providence, RI; Boston; Washington, DC; Baltimore, and Philadelphia. Joe Kolshak, Delta's executive vice president for operations, said the canceled flights made up about a third of Delta's departures and arrivals in the Northeast on Thursday. He said Delta trimmed the flights after the Federal Aviation Administration alerted airlines Thursday it would slow air traffic in the region because of forecasts of heavy rain and lightning. Kolshak said the leaner schedule would reduce delays among the remaining Delta flights.

Source: [http://www.usatoday.com/travel/flights/2007-06-28-delta-cancel\\_N.htm](http://www.usatoday.com/travel/flights/2007-06-28-delta-cancel_N.htm)

17. *June 29, Associated Press* — **Bus with diverted air passengers crashes.** A tour bus carrying diverted airline passengers crashed on an interstate exit ramp early Friday, June 29, killing the driver and injuring a dozen passengers. The bus was trying to exit the southbound lanes of I-81 in northeastern Pennsylvania when it crashed through several barriers, crossed the ramp and landed with part of the vehicle hanging off the roadway, according to state police. The cause of the crash remained under investigation. The bus driver died at the scene. Twelve passengers were taken to hospitals by ambulances, but airline officials said their injuries were not believed to be serious. The passengers had been among about 170 people on a flight from Salt Lake City to Newark, N.J., that was diverted to Syracuse, NY, because of bad weather Thursday night, said Brian Drake, a spokesperson for Delta Air Lines Inc., in Syracuse. After the plane landed, mechanics discovered a hydraulic leak that could not immediately be fixed, Drake said. The airline was unable to find hotel rooms for the passengers, so it called in seven tour buses, which left for Newark around 2:30 a.m. EDT.

Source: [http://hosted.ap.org/dynamic/stories/B/BUS\\_ACCIDENT?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/B/BUS_ACCIDENT?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT)

18. *June 29, USA TODAY* — **Airlines begin recovery after week of cancellations, delays.** Airlines are starting to recover from widespread weather-related delays and cancellations over the past week, but the combination of the passenger backlog and packed Fourth of July holiday flights will cause some travelers to wait days. Over the last week, airlines canceled, delayed and diverted thousands of flights due to bad weather in the Northeast, Midwest, Florida, and Texas. Restrictions on flight crews' monthly hours made things worse as June nears an end. On Thursday, Delta canceled 200 flights, or about a third of its Northeast flights including those

operated by its regional partner Comair, because of heavy storms and expected delays at airports in New York, Philadelphia and Boston. Delta said it cancelled the flights early to notify passengers through e-mail and cell phone messages well ahead of travel time. "We're working very hard to re-accommodate those passengers on other flights throughout the weekend," says Chris Kelly, a spokesperson for Delta Air Lines. For the majority of affected travelers, the schedule changes meant getting home slightly later than they'd originally expected. But some sat on boarded planes for hours, flew to an alternate city where the airline didn't normally operate or got stranded away from home for several days.

Source: [http://www.usatoday.com/travel/flights/2007-06-29-delays\\_N.htm](http://www.usatoday.com/travel/flights/2007-06-29-delays_N.htm)

19. *June 29, Associated Press* — **EU, U.S. agree on sharing air passenger data.** A new airline passenger information sharing agreement between the European Union (EU) and the United States aimed at thwarting terrorism will likely go into effect by July following concessions from both sides this week. Envoys from the EU's 27 nations reached a "basic political understanding" on the new deal, which was struck Wednesday, June 27, by EU and U.S. negotiators, the German EU presidency said. Under the new deal struck Wednesday by German Interior Minister Wolfgang Schauble, EU Justice Commission Franco Frattini and U.S. Department of Homeland Security Secretary Michael Chertoff, the number of pieces of information transferred to U.S. authorities will be reduced from 34 to 19. Those recorded data pieces — such as passenger names, addresses, seat numbers and credit card and travel details — are transferred to U.S. authorities within 15 minutes of a flight's departure for the United States under Washington's anti-terror screening rules. Data can be kept for a maximum of 15 years, but after the first seven years it will become "dormant" and can only be accessed on a case-by-case basis under strict rules.

Source: [http://www.usatoday.com/travel/flights/2007-06-29-passenger-data\\_N.htm](http://www.usatoday.com/travel/flights/2007-06-29-passenger-data_N.htm)

20. *June 29, Associated Press* — **Man charged with intimidation on flight.** A Jet Blue Airlines flight was diverted from its original flight plan after a passenger became irate when the crew refused to serve him more alcohol, Department of Justice officials said Friday, June 29. Jose Roman, 26, was arrested by the FBI Thursday and charged with assaulting and intimidating flight crew and with interfering with the ability of flight crewmembers and flight attendants to perform their duties, said U.S. Attorney Terrance Flynn in a written statement. Roman was on Flight 622 from George Bush International Airport in Houston en route to John F. Kennedy Airport in New York, when the flight was diverted to Buffalo/Niagara International Airport. Assistant U.S. Attorney James Kennedy, Jr., said in a written statement that Roman made statements to the crew and other passengers that he was going to shoot and kill the flight crew when the plane landed in New York. If found guilty, he faces up to 20 years in prison, a fine of \$250,000, or both.

Source: [http://biz.yahoo.com/ap/070629/ny\\_brf\\_flight\\_intimidation.html?v=1](http://biz.yahoo.com/ap/070629/ny_brf_flight_intimidation.html?v=1)

[[Return to top](#)]

## **Postal and Shipping Sector**

Nothing to report.

[[Return to top](#)]



## Agriculture Sector

Nothing to report.

[[Return to top](#)]

## Food Sector

**21. *June 28, U.S. Food and Drug Administration* — FDA warns consumers not to eat Veggie Booty snack food.** The U.S. Food and Drug Administration (FDA) is warning consumers not to eat Veggie Booty snack food, marketed by Robert's American Gourmet, due to possible contamination with Salmonella Wandsworth. Individuals who have recently eaten Veggie Booty and who have experienced any of the symptoms described below should report it to state or local health authorities. This warning is based on 52 reports of illness across 17 states, beginning in March 2007. Almost all the illnesses have occurred in children under 10 years old, with the most cases in toddlers. Most persons had reported bloody diarrhea; four were hospitalized. FDA learned of the illnesses on June 27 from the U.S. Centers for Disease Control and Prevention, which conducted an investigation of the illnesses with state and local health officials. The outbreak is considered likely to be ongoing. States reporting illnesses include: California (seven cases), Colorado (five cases), Connecticut (one case), Georgia (one case), Indiana (one case), Massachusetts (three cases), Minnesota (two cases), New Hampshire (two cases), New Jersey (two cases), New York (13 cases), Oregon (one case), Pennsylvania (three cases), Tennessee (one), Texas (one), Vermont (three cases), Washington (four cases), and Wisconsin (two cases).

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01661.html>

**22. *June 28, U.S. Food and Drug Administration* — FDA detains imports of farm-raised Chinese seafood.** The U.S. Food and Drug Administration (FDA) Thursday, June 28, announced a broader import control of all farm-raised catfish, basa, shrimp, dace (related to carp), and eel from China. FDA will start to detain these products at the border until the shipments are proven to be free of residues from drugs that are not approved in the U.S. for use in farm-raised aquatic animals. This action by FDA will protect American consumers from unsafe residues that have been detected in these products. There have been no reports of illnesses to date. During targeted sampling from October 2006 through May 2007, FDA repeatedly found that farm-raised seafood imported from China were contaminated with antimicrobial agents that are not approved for this use in the U.S. The contaminants were the antimicrobials nitrofurans, malachite green, gentian violet, and fluoroquinolone. Nitrofurans, malachite green, and gentian violet have been shown to be carcinogenic with long-term exposure in lab animals. The use of fluoroquinolones in food animals may increase antibiotic resistance to this critically important class of antibiotics. None of these substances is approved for use in farm-raised seafood in the U.S., and the use of nitrofurans and malachite green in aquaculture is also prohibited by Chinese authorities.

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01660.html>

**23. *June 28, Associated Press* — Japan to examine U.S.-submitted data on American beef imports.** Japan and the U.S. wrapped up two-day talks Thursday, June 28, after exchanging technical views and data on American beef imports but there was no agreement on

Washington's calls for Tokyo to relax its import restrictions, officials said. Japan only allows imports of U.S. beef from cattle 20 months old or younger, because mad cow disease has not been detected in meat from young cattle. In May, the World Organization for Animal Health ruled that the U.S. was a "controlled risk nation" — a country that can export beef from cattle of any age. The U.S. has cited that report in urging Japan to review its policy. During the closed, technical meeting, the U.S. submitted the data it provided to the animal health organization, and Japan will examine them, Agriculture Ministry official Toshio Katagai said. Katagai said the talks focused on cattle feed and the surveillance system in the U.S. Japanese experts also requested further details about them, to be submitted later by the U.S.

Source: <http://www.iht.com/articles/ap/2007/06/28/asia/AS-GEN-Japan-US-Beef.php>

24. *June 28, Associated Press* — **South Korea to inspect beef facilities in U.S.** South Korea said Thursday, June 28, it will conduct on-site inspections of beef industry facilities in the U.S. this weekend ahead of talks about further easing Seoul's restrictions on imports of American beef. An eight-member government delegation will visit cattle ranches, slaughter houses and animal feed facilities to check the sanitary condition of American beef from Saturday through July 8, the Ministry of Agriculture and Forestry said in a statement. The inspection is part of an eight-stage risk assessment South Korea has conducted in a possible step toward resuming imports of meat attached to bone, which is currently banned. Seoul has said the process could be wrapped up as early as September if things go smoothly.

Source: <http://www.businessweek.com/ap/financialnews/D8Q1LVEG1.htm>

[[Return to top](#)]

## **Water Sector**

25. *June 30, Associated Press* — **Lake Okeechobee water levels keep dropping.** Water managers reported Saturday, June 30, that the lake's water level reached a record low of 8.88 feet above sea level, passing the previous mark of 8.89 feet set June 1. The lake is the main backup water supply for five million South Florida residents. Conditions have been so dry in central Florida that water has not flowed from the Kissimmee River into the lake in more than seven months. The drought has forced stringent water restrictions on homes and businesses, and four coastal wells were closed to prevent saltwater contamination.

Source: <http://www.jacksonville.com/apnews/stories/063007/D8Q387901.shtml>

26. *June 30, News 8 (TX)* — **Flood cripples Marble Falls' water system.** Marble Falls, TX's water supply is completely crippled because of damage from floods of water in the past few days. People can't use the system's water, even if they boil it. The city has enacted the same water restrictions as they would in a severe drought. All non-essential water use is prohibited. People are relying on bottled water donated by the Red Cross for drinking and cooking. Restaurants and hair and nail salons served by the Marble falls water system have been shut down. The city is working on the problem, but full water pressure isn't expected to be up for several more days.

Source: [http://www.news8austin.com/content/your\\_news/default.asp?ArID=187208](http://www.news8austin.com/content/your_news/default.asp?ArID=187208)

27. *June 29, Associated Press* — **Cleaning supply manufacturer pleads guilty to environmental**

**violations.** An Atlanta, GA, cleaning product manufacturer was fined \$3.8 million and ordered to serve three years probation after pleading guilty on Friday, June 29, to violating the Clean Water Act. Daniel Schaffer, the company's former director of environmental compliance, pleaded guilty to violating the Clean Water Act in February 2006 and is awaiting sentencing. Among the violations Acuity was accused of, federal prosecutors said that beginning as early as September 1998 and continuing until November 2002, Acuity submitted false information on its wastewater flow, phosphorous output and pH levels to the Atlanta wastewater treatment facility. The company also failed to report significant discharges to the city, including a 10,000-gallon phosphorous discharge in April 2000 and an acid spill in March 2002.

Source: <http://www.ledger-enquirer.com/251/story/73141.html>

[[Return to top](#)]

## **Public Health Sector**

### **28. *July 01, United Press International* — Respiratory tularemia treatment created.** U.S.

researchers have developed a technique that has experimentally protected laboratory mice from developing respiratory tularemia. The respiratory form of tularemia, a potentially serious bacterial disease, is a highly infectious disease with a high mortality rate if untreated. It is also considered a potential bioterrorism tool. Researchers discovered treating laboratory mice with a serum containing tularemia-specific antibodies protects the mice against *F. tularensis*, not only if given before exposure to lethal doses of inhalational *F. tularensis*, but also up to 48 hours after exposure.

Abstract: [http://www.jimmunol.org/cgi/content/abstract/179/1/532?maxto show=&HITS=10&hits=10&RESULTFORMAT=&fulltext=tularemia&searchid=1&FIRSTINDEX=0&volume=179&issue=1&resourcetype=HWCIT](http://www.jimmunol.org/cgi/content/abstract/179/1/532?maxto%20show=&HITS=10&hits=10&RESULTFORMAT=&fulltext=tularemia&searchid=1&FIRSTINDEX=0&volume=179&issue=1&resourcetype=HWCIT)

Source: <http://www.sciencedaily.com/upi/index.php?feed=Science&article=UPI-1-20070628-12323100-bc-us-tularemia.xml>

### **29. *June 28, Reuters* — Czech, German bird flu have same origin.** The deadly strains of bird flu that has killed birds in the Czech Republic and southern Germany are similar and most likely have a common origin, Germany's top state veterinary laboratory said on Thursday, June 27. The Czech Republic reported finding the deadly H5N1 strain of avian influenza virus at two poultry farms and in a dead swan. Germany has found the virus in a number of wild birds in the eastern state of Saxony and southern state of Bavaria. Germany's Friedrich Loeffler Institute said it compared the viruses found in a wild swan near the Bavarian city of Nuremberg with samples from a Czech turkey farm and found that they had a 99.2 percent match.

Source: <http://www.alertnet.org/thenews/newsdesk/L28852930.htm>

### **30. *June 27, Dallas Morning News* — CDC probes bioweapons infections.** Federal authorities are investigating two cases from last year in which Texas A&M researchers were infected with biological weapons agents — including the university's failure to report the exposures when they happened. New documents obtained by The Sunshine Project, a bioweapons watchdog group, show three researchers tested positive for exposure to the weapons agent Q fever in April 2006, two months after another researcher fell ill following contact with the agent *Brucella*. In neither case did university officials immediately report the exposures to the U.S. Centers for Disease Control and Prevention (CDC), as federal law requires. They filed a report

on the Brucella case a year after the initial infection, and CDC officials said Tuesday, June 26, that they still haven't received documentation on the Q fever case.

Source: <http://www.dallasnews.com/sharedcontent/dws/news/texasouthwest/stories/062707dntexinfect.37922e4.html>

[[Return to top](#)]

## **Government Sector**

31. *June 29, Mansfield News Journal (OH)* — **Sheriff: Mercury spill no accident.** Someone intentionally brought mercury into Ohio's Morrow County Courthouse on Wednesday, June 27, according to the agency leading the investigation. "We believe it was an intentional act," said Morrow County Sheriff Steve Brenneman. "There is a person of interest being pursued ... Preliminary viewing of video indicates a potential subject of interest. Brenneman's office is working with the Ohio Environmental Protection Agency, the Bureau of Criminal Identification and Investigation in Columbus and the Morrow County Homeland Security office. "The investigation is still open and we hope to have more answers in the next 24 hours," said Morrow County Prosecutor Charles Howland. "The circumstances are very strange." As the cleanup at the courthouse continues, investigators have been collecting evidence. The courthouse will be closed through the weekend. Cleanup is being run by Ohio EPA. The spill, estimated to be approximately a pound or more of mercury, was first discovered by courthouse employees.

Source: <http://www.mansfieldnewsjournal.com/apps/pbcs.dll/article?AI=D=/20070629/NEWS01/706290316/1002>

32. *June 28, Government Accountability Office* — **GAO-07-1041T: Homeland Security: Transforming Departmentwide Financial Management Systems Remains a Challenge (Testimony).** Since 2003, when the Department of Homeland Security (DHS) began operations, it has faced the difficult challenge of bringing together 22 diverse agencies and developing an integrated financial management system to provide reliable, timely, and useful financial information. The Government Accountability Office's (GAO) 2007 report, *Homeland Security: Departmentwide Integrated Financial Management Systems Remain a Challenge*, GAO-07-536, emphasized the key issues related to DHS attempting to transform its financial management systems. For today's hearing, this testimony, based on GAO's recent report, (1) summarizes DHS's financial system transformation efforts, (2) points out key financial system transformation challenges at DHS, and (3) highlights the building blocks that DHS should consider to form the foundation for successful financial management system transformation efforts. Though there are no recommendations in this statement, in its related report (GAO-07-536), GAO made six recommendations focused on the need for DHS to define a departmentwide financial management strategy and embrace best practices, including human capital practices, to foster its systems integration effort. DHS concurred with GAO's recommendations.

Highlights: <http://www.gao.gov/highlights/d071041thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-1041T>

33. *June 21, Government Accountability Office* — **GAO-07-536: Homeland Security: Departmentwide Integrated Financial Management Systems Remain a Challenge**

**(Report).** Since the Department of Homeland Security (DHS) began operations in March 2003, it has faced the daunting task of bringing together 22 diverse agencies and developing an integrated financial management system to provide timely, reliable, and useful financial information. The Government Accountability Office (GAO) was asked to determine (1) whether DHS has fully developed plans for implementing and/or migrating to an integrated departmentwide financial management system, (2) the potential usefulness of the work products received for the funds spent on the financial modernization effort, and (3) going forward, how DHS can incorporate best practices into its plans for migrating to an integrated departmentwide financial management system. GAO interviewed key DHS officials, reviewed relevant DHS policy and procedure documents, and analyzed work products related to the financial modernization effort. To help reduce the risks associated with a departmentwide financial management system implementation effort, GAO makes six recommendations focused on the need for DHS to define a departmentwide financial management strategy and embrace best practices to foster systems development, including key human capital practices. DHS concurred with GAO's recommendations.

Highlights: <http://www.gao.gov/highlights/d07536high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-536>

[\[Return to top\]](#)

## **Emergency Services Sector**

34. *June 28, GovExec* — **Locals question DHS decision to ditch communications project.** The Department of Homeland Security's (DHS) effort to scrap a digital communications tool used to coordinate emergency response with local governments has riled a group of county-level officials. In a June 18 memorandum, Timothy Loewenstein, chairman of the information technology committee at the National Association of Counties, told the DHS technology chief that discontinuing or diminishing the Disaster Management program without talking to the users was unacceptable. Disaster Management's mission is to create interoperable communication standards for emergency management software and to distribute free basic disaster management software to local governments that otherwise could not afford to buy such tools.

Source: [http://www.govexec.com/story\\_page.cfm?articleid=37323&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=37323&dcn=to daysnews)

35. *June 28, Computer World* — **University of Florida building device that simulates hurricanes.** The University of Florida is constructing a portable machine that can simulate intense weather conditions for researchers trying to better understand how building components react to hurricane force winds and rain. The massive hydraulic fuel-powered device will simulate the impact of hurricane-strength winds and rain on windows, doors, roofs and other building components made of timber and masonry products, said Forrest Masters, assistant professor in the department of civil and coastal engineering at the University of Florida in Gainesville. Masters said the \$500,000 project aims to help researchers better "uncover the origin and path of water intrusion and to innovate new products that ultimately make homes more resilient during hurricane landfalls." Once testing of the machine is completed, it will be rolled out in the field to test the mettle of vacant homes and structures donated to the cause by the state.

Source: <http://www.computerworld.com/action/article.do?command=viewA>



36. *June 27, Government Technology* — **U.S. Fire Administration announces Web-based online training system.** The U.S. Fire Administration's National Fire Academy is pleased to announce the launch of a new Web-based online training system, NFAOnline. The Website provides an easy, one-stop site where fire and emergency services personnel, first responders, emergency management personnel, and the general public will find free training and education programs that they can complete at their own pace. NFAOnline provides a user-friendly, state-of-the-art training system with technical support and the ability for the student to immediately print a certificate and transcript. The primary effort of NFAOnline is to make available training and materials for the fire service, particularly those unable to attend resident courses in Emmitsburg, MD.

NFA Online Website: <http://www.nfaonline.dhs.gov/>

Source: <http://www.govtech.com/gt/articles/125858>

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

37. *June 29, IDG News Service* — **Department of Homeland Security to host closed-door security forum.** The Department of Homeland Security will host an invite-only conference two months from now that will bring together security experts from law enforcement, Internet service providers, and the technology industry. The Internet Security Operations and Intelligence (ISOI) workshop will be held on August 27 and 28 at the Academy for Educational Development in Washington, DC. It is expected to draw about 240 participants who will engage in a frank discussion of the latest trends in cybercrime, said Gadi Evron, a security evangelist with Beyond Security who is one of the event's planners.

Source: [http://news.yahoo.com/s/infoworld/20070629/tc\\_infoworld/8978](http://news.yahoo.com/s/infoworld/20070629/tc_infoworld/8978)

6: [ylt=AtPrh6pqrZCNUmledgz4pAcjtBAF](#)

38. *June 29, IDG News Service* — **Microsoft.co.uk succumbs to SQL injection attack.** A hacker successfully attacked a Webpage within Microsoft's UK domain on Wednesday, June 27, resulting in the display of a photograph of a child waving the flag of Saudi Arabia. It was "unfortunate" that the site was vulnerable, said Roger Halbheer, chief security advisor for Microsoft in Europe, the Middle East and Africa, on Friday. The problem has since been fixed. However, the hack highlights how large software companies with technical expertise can still prove vulnerable to hackers. The hacker, who posted his name as "rEmOtEr," exploited a programming mistake in the site by using a technique known as SQL injection to get unauthorized access to a database, Halbheer said.

Source: [http://news.yahoo.com/s/infoworld/20070629/tc\\_infoworld/8979](http://news.yahoo.com/s/infoworld/20070629/tc_infoworld/8979)

5: [ylt=Ai0coEUBCqNCNVAA5T1W\\_sQjtBAF](#)

39. *June 28, IDG News Service* — **RealPlayer, Helix Player vulnerable to attack.** Users are being advised to upgrade to newer versions of the RealPlayer and Helix Player multimedia products because of a critical security flaw. The flaw could allow an attacker to gain control over a user's PC using a buffer overflow vulnerability, a memory problem that can allow

unauthorized code to run on a machine, according to iDefense Inc. The vulnerability was discovered last October but publicly disclosed Tuesday, June 26, on iDefense's Website. Affected versions of the software include the 10.5 "gold" RealPlayer and any 1.x version of Helix Player, according to the French Security Incident Response Team (FrSIRT). iDefense advisory: <http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=547> Source: [http://www.infoworld.com/article/07/06/28/RealPlayer-Helix-Player-vulnerable\\_1.html](http://www.infoworld.com/article/07/06/28/RealPlayer-Helix-Player-vulnerable_1.html)

**40. *June 28, ComputerWorld* — Web-based attack poses as greeting card, tries three exploits.**

A new round of greeting-card spam that draws users to visit attack sites relies on a sophisticated multipronged, multiexploit strike force to infect machines, security professionals said late Thursday, June 28. Captured samples of the unsolicited e-mail have all borne the same subject line — "You've received a postcard from a family member!" — and contain links to a malicious Website. "If JavaScript is disabled, then they provide you a handy link to click on to exploit yourself," said an alert posted Thursday afternoon by SANS Institute's Internet Storm Center (ISC). The greeting-card gambit tries a trio of exploits, moving on to the second if the machine is not vulnerable to the first, then on to the third if necessary. The first is an exploit against a QuickTime vulnerability; the second is an attack on the popular WinZip compression utility; and the third, dubbed "the Hail Mary" by the ISC, is an exploit for the WebViewFolderIcon vulnerability in Windows that Microsoft Corp. patched last October. The ISC said several antivirus vendors had tentatively pegged the executable file, which is offered to users whose browsers have JavaScript disabled, as a variation of the Storm Trojan horse. ISC alert: <http://isc.sans.org/diary.html?storyid=3063> Source: [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025898&intsrc=hm\\_list](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025898&intsrc=hm_list)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

- 41. *June 30, Associated Press* — Los Angeles: 2,500 pounds of fireworks found in home.** A man was arrested after authorities found 2,500 pounds of illegal fireworks at his home, officials said Friday, June 29. George Stoner Carrera, 47, was arrested Thursday, June 28, at his home in Los Angeles for investigation of possessing unlawful explosives, said Scott Burnside, an arson investigator with the Alhambra Fire Department. The fireworks — enough to fill two flatbed trucks and worth at least \$25,000 — were transported from Nevada and stored throughout the house. They included nearly 2,000 black, powder-filled M-80 explosives, which are considered illegal explosive devices in California, Burnside said. "This is a matter of public safety," Burnside said. "I've worked every Fourth of July and every year I see fires."

Source: [http://hosted.ap.org/dynamic/stories/B/BRE\\_FIREWORKS\\_RAID?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/B/BRE_FIREWORKS_RAID?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT)

- 42. June 29, CNN — New York chemicals intended for resale, police say.** A man who allegedly stored nearly 1,500 pounds of potassium nitrate and other chemicals in his Staten Island home and a nearby storage facility was charged with reckless endangerment Friday, June 29, according to the New York City Police Department. Police said Miguel Serrano, 57, had bought the chemicals in bulk from an Ohio-based dealer and was intending to resell the chemicals in smaller quantities on the Internet. It was the dealer who tipped off the Bureau of Alcohol, Tobacco, Firearms and Explosives after Serrano had allegedly ordered 5,000 pounds of potassium nitrate. Late Thursday night, several residential blocks were cordoned off and a few dozen homes were evacuated in Staten Island as police searched Serrano's home and a nearby commercial storage facility. According to New York Police Department (NYPD) Sgt. Kevin Hayes, authorities found less than a thousand pounds of chemicals in the home, including potassium nitrate, sulfur, mercury, and peroxide. At the off-site storage facility, authorities found about 1,500 pounds of chemicals, mainly potassium nitrate. The NYPD said there is no indication the chemicals were being used for bomb making or anything terror-related.

Source: <http://www.cnn.com/2007/US/06/29/chemicals.found/index.html>

[\[Return to top\]](#)

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983-3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

**Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.